ECC-based User Authentication Scheme for Wireless Sensor Networks

Imanbaev Temirlan[1], Yue Li[2]

School of Computer Science and Technology, Donghua University, No. 2999 North Renmin Road, Songjiang, Shanghai 201620, China

Abstract**—** *In 2016, Akansha S. et al. proposed an upgraded user authentication protocol. According to the implemented cryptanalysis on their scheme, some vulnerabilities have been found in registration and authentication part. In registra-tion part, the gateway uses generated value as secrecy and sends it to sensor node, which doesn't have infor-mation about received secret value and cannot verify its identity. In authentication part, user is unable to check legiti-macy of received session key generated by sensor node. Mainly, the protocol has been implemented using only one way hash function, XOR and concatenation operations, which is not adequate to provide authentication and confidentiality. In this paper, we suggest ECC-based user authentication scheme for WSNs, which eliminates the drawbacks of the previous scheme. The protocol decreases the high cost public-key operations of the sensor node and substitutes them with symmetric-key based operations.*

Keywords**— Authentication, Cryptography, Key agreement, Network security, WSN.**

I. INTRODUCTION

Nowadays, the Wireless Sensor Networks becomes a rich sphere of active research containing programming models, distributed algorithms, routing protocols, signal processing, system design, data management and security. For most of the WSN's applications, security is a major concern. Therefore, the resource constraint and computational limitations compels security solutions in WSNs to be differ from standard networks [1]. Sensor nodes are limited in terms of con-suming power, energy levels and memory size. Thus, comparing with wired sensors, the nodes in WSNs have a vulnera-bility to various passive and active attacks. It makes security to be an essential factor for WSNs, where data integrity is the most important requirement. Authentication has three major classes based on the primary cryptographic methods such as asymmetric cryptography, symmetric cryptography and hybrid methods [2]. Initially, it was estimated that WSNs would compose only of equal sensor nodes. But nowadays we are discussing heterogeneous WSNs since sensor networks can be constructed with different kind of nodes, some of them equipped with better computational power comparing with others (e.g. gateway nodes) [3]. The main security requirements for WSNs are authentication, confidentiality, integrity, authorization, non-repudiation, availability and freshness. User identification can be performed using three factors such as physical attributes (for instance fingerprint, retinal pattern etc.), documents and credentials (like smart card, id card etc.), personal information or password [4].

In our work, we clearly show that Akansha S. et al.'s [5] user authentication scheme has some drawbacks, which does not provide resistance against some attacks and is not enough secure. Also, we demonstrate that their scheme can be made much efficient by using ECC and removing some unnecessary steps. To eliminate the weaknesses and improve previous work, we suggest ECC-based user authentication scheme for wireless sensor networks which is more secure as compared to previous work.

The remainder of this paper is arranged as follows. Section 2 describes related works. Section 3 contains a brief review of Akansha et al.'s scheme. The weaknesses of Akansha et al.'s scheme are described in Section 4. In Section 5, some preliminaries and network model are reviewed. Section 6 represents our key agreement protocol. The security of the proposed protocol is discussed in Section 7. We provide our research conclusions in Section 8.

II. RELATED WORK

In this section, we have analyzed some of the related schemes which are proposed in the literature. In 2006, Wong et al. [6] presented his lightweight authentication scheme. But, it has been discovered that their scheme has several weak-nesses against such attacks as forgery, replay and stolen-verifier attack. In 2009, Das et al. [7] improved Wong et al.'s scheme and proposed a two-factor secure authentication protocol for WSNs. Later Das et al.'s scheme was upgraded by some researchers. He et al. [8] proved that Das et al. protocol has some security pitfalls of impersonation attack since it doesn't provide easy password update facility. They offered an improved two-factor hash function protocol, which requires just three message

exchanges for user authentication. Chen et al. [9] also highlighted that Das et al. pro-tocol is not provided by mutual authentication between the gateway and sensor node. In 2010, Khan and Alghathbar [10] offered some enhancements in Das et al.'s scheme. They used password's hash value to get a high password security and pulled out a new idea of pre-shared keys between sensor nodes and the gateway. In 2011, Yeh et al. [11] mentioned that Chen et al.'s scheme doesn't provide easy password update phase, has no resistance against insider attack and suggested an ECC–based user authentication scheme.

In 2013 Shi et al. [12] presented a new user authentication protocol, which eliminates the vulnerability of Yeh et al.'s protocol and which is more efficient in terms of communication, security and computation cost. In 2014, Choi et al. [13] highlighted that Shi et al.'s scheme is sensitive to some security flaws such as stolen smart card attacks, sensor node energy exhausting attack and session key attack. Later, Anup K.M. et al. [4] pointed out several weaknesses in Choi et al.'s scheme. During the analysis, they discovered that the proposed scheme is vulnerable against stolen smart card attack, insecure to sensor node energy exhausting attack and doesn't provide resistance against node capture attack. Afterward, Turkanovic et al. [3] suggested a scheme for mutual authentication, which was discovered as non-secure protocol with many issues by Akansha S. et al.'s. They mentioned that the proposed scheme is not secure against session key recovery attack, reply attack, impersonate attack and offline password guessing attack.

III. REVIEW OF AKANSHA S. ET AL.'S SCHEME

In this section, we did a short review for the Akansha S. et al.'s user authentication protocol. Their scheme contains three entities: the user, the sensor node and the gateway. For Akansha S. et al.'s scheme, there are three phases: registration phase, login phase, authentication and password changing phase.

TABLE 1
NOTATIONS

Symbol	Definition
U_i	User
SC	Smart card
S_j	j_{th} Sensor Node
ID_i	i_{th} User's identity
ID_{sj}	j_{th} Sensor node's identity
PW_i	i_{th} User's password
PW_{sj}	j_{th} Sensor node's password
GW	Gateway
K_{GW}	Secure password known only to Gateway Node
K_{GW-U}	Gateway's secret password key shared with the user U_i
K_{GW-S}	Gateway's secret password key shared with the sensor node j
T	Timestamp
SK	Separately computed session key with private information of both user and sensor node
$\oplus$, ‖, h(.)	XOR, concatenation, lightweight one way hash function

Initially, each user and sensor node has their own identities (ID_i, ID_{sj}) and secret passwords (PW_i, PW_{sj}). The gateway has both entities' identity and password. From the beginning, gateway creates a random key K_{GW-u} and K_{GW-S} to establish secrecy with user and sensor node.

3.1 Registration Phase

3.1.1 Registration between U_i and GW

The user U_i computes $P_i = h(r_i \parallel \mathrm{h}(PW_i))$ with generated random number r_i and sends message $\{P_i, ID_i, T_{s1}\}$ to the GW, which checks the validity of timestamp $|T_{s1} - T_c| < ||\Delta T$ and computes: $a_i = h(K_{GW-U} \parallel ID_i)$, $b_i = a_i \oplus h(P_i \parallel h(PW_i))$, $c_i = h(a_i \parallel h(PW_i) \parallel ID_i)$. The GW personalizes SC with values $\{ h(.), b_i, c_i, ID_i\}$ and sends through secure channel to U_i, who computes an additional value $d_i = r_i \oplus h(ID_i \parallel PW_i)$ and inputs value $\{ h(.), b_i, c_i, d_i, ID_i\}$ into SC.

3.1.2 Registration between GW and S_j

The sensor node S_j computes $P_{sj} = h(ID_{sj} \parallel \mathrm{h}(PW_{sj}) \parallel T_{s2})$ and sends message $\{P_{sj}, ID_{sj}, T_{s2}\}$ to the GW, which checks the validity of timestamp $|T_{s2} - T_c| < ||\Delta T$ and checks a satisfaction of computed P_{sj}* with P_{sj}. If it satisfies the condition, then GW computes the next values using K_{GW}: $\beta_j = h(K_{GW-s} \parallel ID_{sj})$, $b_{sj} = \beta_j \oplus h(ID_{sj} \parallel h(PW_{sj}))$, $c_{sj} = h(\beta_i \parallel h(PW_{sj}) \parallel ID_{sj} \parallel T_{s3})$. The GW sends message $\{ b_{sj}, c_{sj}, T_{s3}\}$ through public channel to S_j, which verifies validity of received timestamp $|T_{s3} - T_c| < ||\Delta T$, extracts β_j from b_{sj} and computes new value c_{sj}*. S_j checks the satisfaction of c_{sj}* with c_{sj} and stores value β_j

3.2 Login Phase

U_i inserts SC into terminal and inputs the new ID_i* and PW_i*. SC calculates r_i*= $d_i \oplus h(ID_i$*$\parallel PW_i$*), MP_i*= $h(PW_i$*), $P_i = h(r_i$*$\parallel MP_i$*), a_i*= $b_i \oplus h(P_i \parallel MP_i$*), c_i*= $h(a_i$*$\parallel MP_i$*$\parallel ID_i$*) and checks satisfaction of c_i* with c_i. U_i creates random value k_i, calculates $M_1 = k_i \oplus h(a_i \parallel MP_i)$, $M_2 = h(a_i \parallel MP_i \parallel k_i \parallel T_1)$ and sends message $\{M_1, M_2, ID_i, T_1\}$ to the GW through public channel.

3.3 Authentication Phase

The GW checks timestamp $|T_1 - T_c| < ||\Delta T$ of received message from U_i, computes k_i*= $M_1 \oplus h(a_i \parallel h(PW_i))$, M_2*= $h(a_i \parallel h(PW_i) \parallel k_i$*$\parallel T_1)$ and checks satisfaction with received values. GW calculates $y_{ij} = h(a_i \parallel \beta_j \parallel ID_i \parallel ID_{sj})$, $M_3 = a_i \oplus y_{ij}$, $M_4 = h(y_{ij} \parallel M_3 \parallel ID_i \parallel T_2)$ and sends message $\{M_4 \parallel M_3 \parallel ID_i \parallel T_2\}$. $U_i$verifies validity of timestamp $|T_2 - T_c| < ||\Delta T$, computes y_{ij}*= $a_i \oplus M_3$, M_4*= $h(y_{ij} \parallel M_3 \parallel ID_i \parallel T_2)$ and checks satisfaction with received values. GW calculates $M_5 = k_i \oplus h(\beta_j \parallel ID_{sj})$, $M_6 = \beta_j \oplus y_{ij}$, $M_7 = h(y_{ij} \parallel k_i \parallel ID_{sj} \parallel T_3)$ and sends message $\{M_5 \parallel M_6 \parallel M_7 \parallel ID_{sj} \parallel ID_i \parallel T_3\}$ to S_j, which checks validity of timestamp $|T_3 - T_c| < ||\Delta T$, computes k_i*= $M_5 \oplus h(\beta_j \parallel ID_{sj})$, $y_{ij} = \beta_j \oplus M_6$, M_7*= $h(y_{ij} \parallel k_i$*$\parallel ID_{sj} \parallel T_3)$ and compares value M_7* with received one. S_j chooses random nonce k_j and calculates $M_8 = k_j \oplus y_{ij}$, $M_9 = h(k_j \parallel ID_{sj} \parallel T_4)$. Finally, S_j computes session key $SK = h(k_i \oplus k_j)$ and sends message $\{M_8 \parallel M_9 \parallel IDi \| IDsj \| T4\}$ to Ui, who verifies validity of received timestamp $|T3-Tc|<|\Delta T$, calculates $kj=M8 \oplus yij$, M_9*= $h(k_j \parallel ID_{sj} \parallel T_4)$, compares value M_9* with received one and computes session key $SK = h(k_i \oplus k_j)$

3.4 Password Changing Phase

U_i inserts SC into terminal and inputs ID_i and PW_i^{OLD}. SC verifies values and asks U_i to choose new password.

IV. SECURITY FLAWS IN AKANSHA S. ET AL.'S SCHEME

To Some weaknesses of Akansha S. et al.'s protocol is detected and analyzed as below:

1) In registration part between the GW and sensor node, GW creates secret value K_{GW-Sj} and hides it inside of β_j. Afterwards, the GW conceals value β_j inside of b_{sj}, c_{sj} and sends message $\{b_{sj}, c_{sj}, T_{s3}\}$ to sensor node, which extracts β_j from b_{sj} computing $\beta_j = b_{sj} \oplus h(ID_{sj} \parallel h(PW_{sj}))$. Due to sensor node doesn't have information about K_{GW-Sj}, which is hidden inside of value β_j, sensor node S_j is not able to determine the identity of GW. So, if an adversary captures GW, then he can creates his own forged secret value K_{GW-Sj} and send to sensor node S_j.

2) In the last step of registration part, user U_i computes additional value $d_i = r_i \oplus h(ID_i \parallel PW_i)$ and puts values $h(.), b_i, c_i, d_i, ID_i$ into smart card. SC already contains values d_i and ID_i. So, to extract value r_i from SC, an attacker only needs to guess value PW_i. Upon r_i is found, an adversary can obtain other values.

3) In authentication part, sensor node S_j calculates session key using generated random value k_j. The GW and user U_i don't know value of k_j or session key. If an adversary captures sensor node S_j and obtains stored value β_j, then he can extract values k_i and y_{ij} from received values sent by the GW. Afterwards, an adversary generates an arbitrary value

k_j and computes session key. Upon user U_i received message from sensor node S_j, he cannot verify identity of k_j or session key value.

4) Generally, in this scheme only hash function, concatenation and XOR functions are employed. Maybe it is the right decision in term of less energy consumption and fast computational speed of sensor nodes. But, we must remember that the first requirement for authentication protocol is security. It is not enough secure to only use hash, concatenation or XOR functions against modern attacks. Because, there are some research works related to attacks on the concatenation and XOR hash combiners [14], [15] have been achieved, which points to their vulnerabilities.

V. REFINED PROTOCOL DESIGN

The IEEE 802.15.4 determines parameters for low-range personal area networks, which was specially designed in terms of providing devices with low speed and low-cost communication. The encryption mechanism pointed in IEEE 802.15.4 standard mainly designed for symmetric key encryption. There are two kinds of devices: a Reduced Func-tional Device (RFD) and a Full Functional Device (FFD). While an RFD acts as a low-power sensor, an FFD acts as a gateway. We model symmetric key based wireless sensor network, which contains some sensor nodes, gateway and user. A gateway authenticates user, computes session key and distributes it to user and sensor node.

VI. PROPOSED SCHEME

We proposed a new ECC-based user authentication scheme for Wireless Sensor Networks, which resolves all the identi-fied weaknesses of Akansha S. et al.'s scheme and ensures high-level security. Our scheme reduces the sensor node's expenses of elliptic curve random point scalar multiplications. We replaced them with low expenses and effective sym-metric-key based operations. In addition, to make our protocol more secure, we combined Elliptic Curve Digital Signa-ture Algorithm (ECDSA) with Message Authentication Code (MAC) for the entities authentication.

TABLE 2
NOTATIONS

Symbol	Definition
U_i	i_{th} User
S_j	j_{th} Sensor Node
SC	Smart card
ID_i	i_{th} User's identity
ID_j	j_{th} Sensor node's identity
PW_i	i_{th} User's password
PW_j	j_{th} Sensor node's password
GW	Gateway
q	a large prime
p	a large prime such that $p = 2q + 1$
P	a base point of large order *n* choosed for an elliptic curve, which is known to all U_i
Q_i, q_i	Public and private key pair of a U_i
Q_v, q_v	Public and private key pair of the powerful node V
$Sig_u(m)$	The signing algorithm based on ECDSA protocols under U_i's private key q_i and the signed message m
$MAC(M,k)$	The calculation of a MAC for a message *m* using MAC key *k*
N_i, N_k	Nonces
T	Timestamp
$\oplus, \|, h(.)$	XOR, concatenation and a lightweight one way hash function
sk	Session key

6.1 Registration Phase

The registration part contains two subparts. The first part is between user and gateway and the second part is between sensor node and the gateway.

6.1.1 Registration between User and Gateway

1) The user U_i chooses his ID_i, PW_i, selects random integer b and computes $pw = h(PW_i \oplus b) * P$

2) U_i creates the pairs of signing and verifying keys (Q_i, q_i) and sends message $\{pw, ID_i, Q_i\}$ to the GW

3) GW stores value Q_i, sets the pair of private and public keys (Q_v, q_v)

4) GW computes $a = h(pw \parallel ID_i) * P$ and sends message $\{a, q_v\}$ to U_i

5) When U_i receives message stores values (a, q_v, b, P) in SC

6.1.2 Registration between Gateway and Sensor Node

1) S_j selects its ID_j, $h(PW_j)$ and generates random number y

2) S_j computes $c = h(ID_j \parallel y)$, $j = h(ID_j \parallel c \parallel h(PW_j) \parallel T_1)$ and sends message $\{j, ID_j, h(PW_j), c, T_1\}$ to the GW

3) GW checks timestamp T_1 and compares received value j with new one.

4) GW calculates $d = h(c \parallel ID_j) * P$, $g = d.x \oplus h(ID_j \parallel h(PW_j))$ where x is the coordinator of d and calculates $f = h(g \parallel T_2)$

5) GW sends message $\{f, g, T_2\}$ to S_j

6) S_j checks timestamp T_2, compares received value d with new one and stores it.

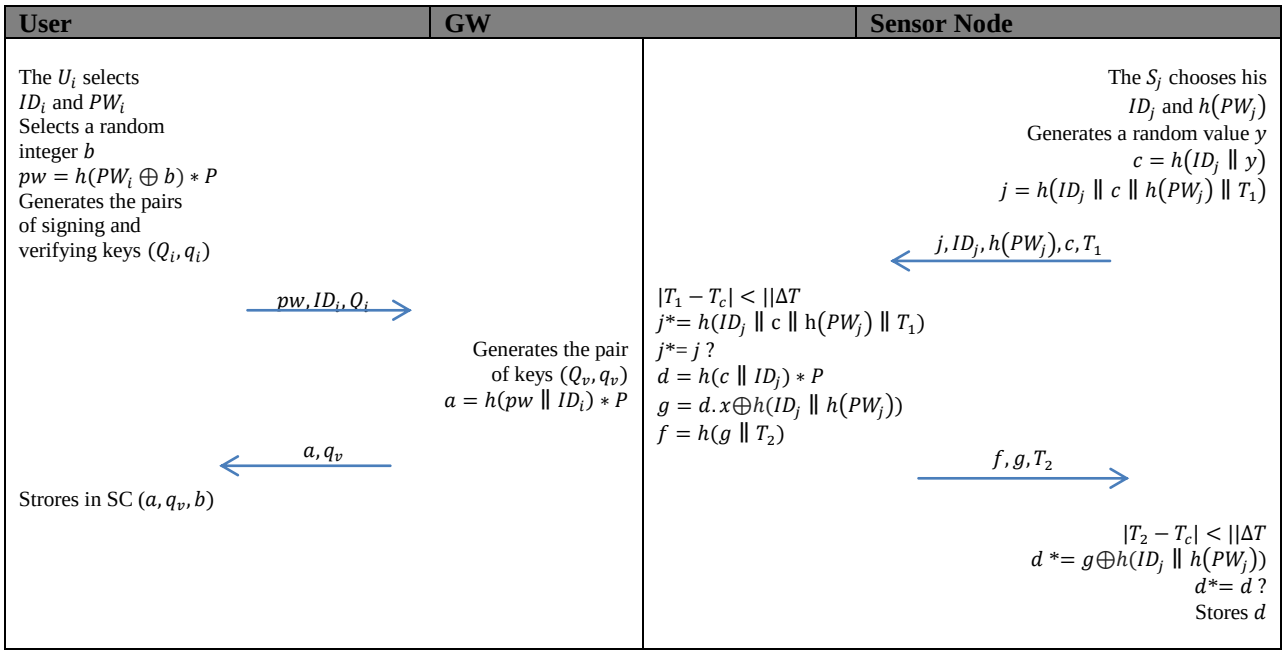

FIGURE 1 REGISTRATION PHASE

6.2 Login and Authentication Phase

After user passed registration phase, he can connect to sensor node via the gateway node.

6.2.1 Login phase

1) U_i inserts SC into terminal, inputs ID_i and PW_i

2) Computes new values $a^* = h(pw \parallel ID_i) * P$ and compares with value taken from SC $a^* = a$?

3) U_i selects random nonce k and N_i, where k is a MAC key

4) U_i computes secret value $R = a * q_v$ and cipher text $w = (k \parallel N_i) \oplus \mathrm{R}.x$

5) Generates an ECDSA signature $s = Sig_u(a \parallel w)$ and sends message $\{s, a, w\}$ to the GW

6.2.2 Authentication phase

1) When the GW receives message from U_i restores secret value $R = h(pw \parallel ID_i) * Q_v$

2) Extracts k from value w

3) Generates random value N_k

4) Computes session key $sk = h(N_k \parallel k)$ and cipher text $e = sk \oplus \mathrm{R}.x$

5) GW first sends message $\{e, MAC(e,k)\}$ to U_i, which upon receiving, verifies MAC and calculates session key $sk = e \oplus \mathrm{R}.x$

6) GW computes $Z = R.x \oplus d.x$ and forwards message $\{pw, e, Z, w\}$ to S_j

7) S_j extracts R from $Z = R.x \oplus d.x$ and computes session key $sk = e \oplus \mathrm{R}.x$

8) S_j extracts k from w and sends message $E(pw.x \parallel N_i, sk), MAC(E(pw.x \parallel N_i, sk), k)$ to U_i

9) U_i verifies MAC, decrypts cipher text and checks satisfaction of received session key value with his own one $sk^* = sk$?

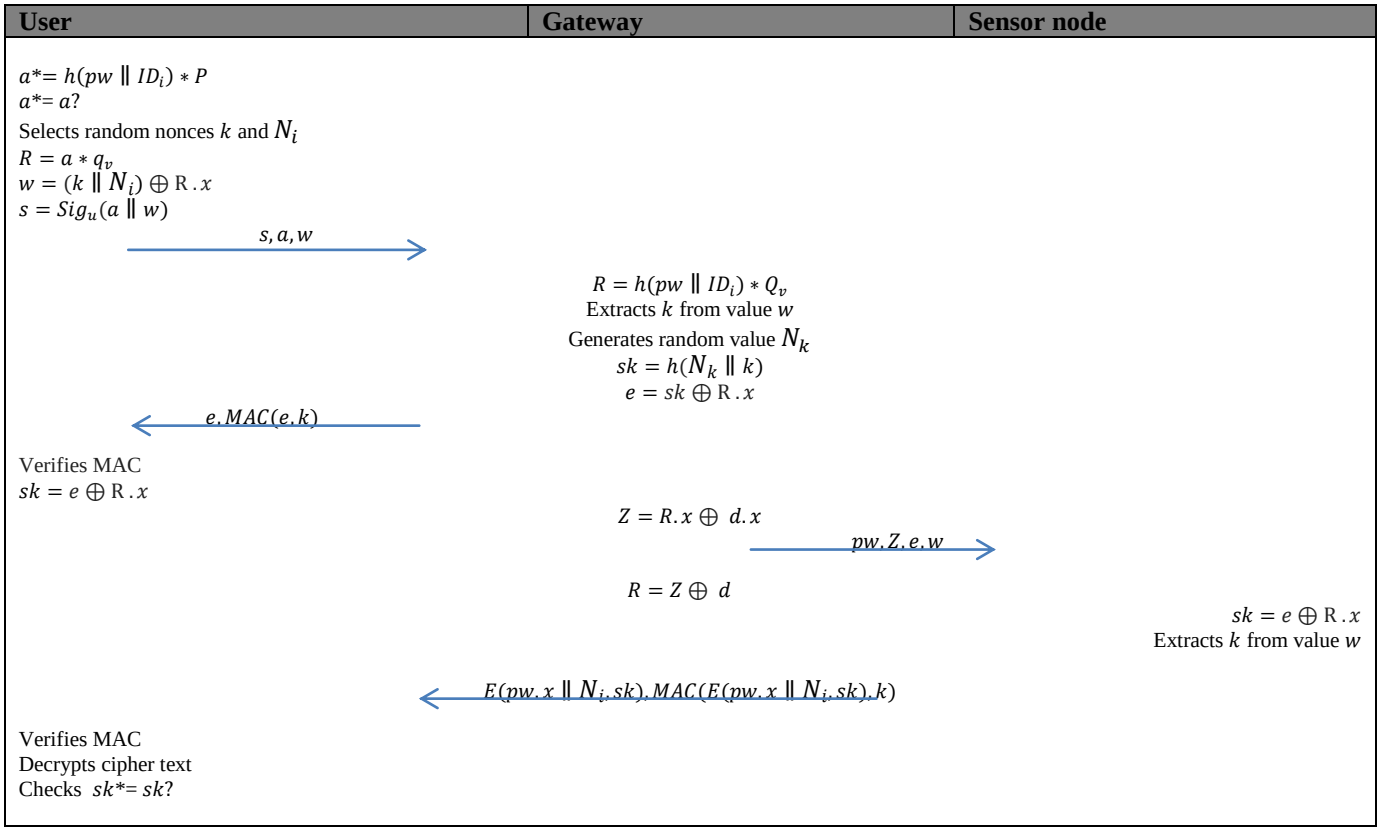

FIGURE 2 LOGIN AND AUTHENTICATION PHASE

VII. SECURITY ANALYSIS

This section provides a security analysis of our work and proves the proposed scheme has resistance to the several attacks and is able to provide a secure authentication.

7.1 Sensor Node Replication Attack

This type of attack, where an attacker generates his own low-cost sensor node called forge node and misinforms the network to affirm them as a legitimate one. To perform this attack, an attacker needs to physically capture one of the nodes and collect all secret values (ID, cryptographic keys and etc.). After that, an attacker duplicates the sensor node and creates one or more

copies of the node into the current network. In terms of avoiding replayed message attack in our protocol, we used a fresh nonce n, which sent by user U_i. If an attacker plans to replay the previously transferred message from user U_i, then he has to use the previously sent n nonce value. Thus, an adversary is not able to reply message, because the GW knows the last nonce value, which was created by user U_i.

7.2 Sybil Attack

Generating different accounts from various IP addresses an adversary pretends himself as multiple forge identities. In terms of resistance against such attack we used ECDSA to create and verify the signature of each user U_i. The attacker cannot pretend as user U_i and pass GW without the private key q_i. Even in worst case, the attacker expose user U_i but still is unable to claim a new identity of user U_i in the neighborhood of user U_j because the attacker only knows the private key of the exposed user U_i but not the private key of user U_j. In fine, due to using ECDSA on the gateway to authenticate the identity of user, the proposed protocol provides withstand the Sybil attack.

7.3 Insider Attack

An insider attack usually appears when the GW or system administrator can have access to a user's credentials and can impersonate user. In our scheme, for the insider of GW node is not possible to get user U_i's password, because the GW only have a value pw, which contains a value b and PW_i. The value b is high entropy value, which is not revealed to the GW. Thus, it is not possible to guess both values of pw.

7.4 Man-in-the-Middle-Attack

An adversary catches the messages being exchanged between the entities and sends forge messages impersonating one of them. Regarding our scheme, the message exchanging between user U_i and GW, performed using signature and MAC key, which allow only to the legal entities authenticate each other.

7.5 Mutual Authentication

Mutual authentication is the main security property for the authentication protocol. In our case, the proposed scheme provides mutual authentication among 2 entities: user and gateway. The signature of the message sent from user U_i to GW provides an authentication of user U_i. Also, a Message Authentication Code will provide evidence of integrity for the message. Because, the MAC key k was generated and encrypted by user U_i. Thus, only GW with private key q_v can recover value k. When GW sends back message, it will use the same MAC key k.

VIII. CONCLUSION

In this paper, Akansha S. et al.'s protocol has been reviewed and analysed. Based on the cryptanalysis of their scheme, have been found some drawbacks. In registration part, the gateway generates new secret value, which is not known to sensor node. Hence, sensor node is unable to check identity of received secret value. Also, there is possibility of smart card breach attack, because the adversary only needs to guess user's password to obtain values from the smart card. In authentication part, sensor node computes session key value and sends to user. It leads to the sensor impersonation attack since user doesn't know value of session key and cannot authenticate sensor node. The general vulnerability of Akansha S. et al.'s scheme is that they only used a hash function, XOR and concatenation. As mentioned above, these operations cannot provide enough security. Comparing to the Akansha S. et al.'s scheme, we have designed a protocol based on the IEEE 802.15.4 standard of network model using ECC. In our scheme, the signature algorithm ECDSA and the Message Authentication Code (MAC) have been implemented, which provides a mutual authentication. Also, in registration part, the scheme provides secure key agreement resistant to the smart card breach attack.

REFERENCES

[1] A. Joux, Multicollisions in iterated hash functions. Application to cascaded constructions, Annual International Cryp-tology Conference, Springer, 2004, pp. 306-316.

[2] A.K. Maurya, V. Sastry, S.K. Udgata, Cryptanalysis and Improvement of ECC-Based Security Enhanced User Authentication Protocol for Wireless Sensor Networks, International Symposium on Security in Computing and Communication, Springer, 2015, pp. 134-145.

[3] A. Singh, A.K. Awasthi, K. Singh, Cryptanalysis and Improvement in User Authentication and Key Agreement Scheme for Wireless Sensor Network, Wireless Personal Communications, 1-18.

[4] A. Tajeddine, A. Kayssi, A. Chehab, I. Elhajj, Authentication schemes for wireless sensor networks, MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference, IEEE, 2014, pp. 367-372.

[5] D. He, Y. Gao, S. Chan, C. Chen, J. Bu, An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Net-works, Ad Hoc & Sensor Wireless Networks, 10 (2010) 361-371.

[6] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, H.-W. Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors, 11 (2011) 4767-4779.

[7] I. Dinur, New Attacks on the Concatenation and XOR Hash Combiners, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2016, pp. 484-508.

[8] K.H. Wong, Y. Zheng, J. Cao, S. Wang, A dynamic user authentication scheme for wireless sensor networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), IEEE, 2006, pp. 8 pp.

[9] M.L. Das, Two-factor user authentication in wireless sensor networks, IEEE Transactions on Wireless Communications, 8 (2009) 1086-1090.

[10] M.K. Khan, K. Alghathbar, Cryptanalysis and security improvements of 'two-factor user authentication in wireless sen-sor networks', Sensors, 10 (2010) 2450-2459.

[11] M. Turkanović, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks, 20 (2014) 96-112.

[12] S. Bartariya, A. Rastogi, Security in Wireless Sensor Networks: Attacks and Solutions, environment, 5 (2016).

[13] T.-H. Chen, W.-K. Shih, A robust mutual authentication protocol for wireless sensor networks, ETRI journal, 32 (2010) 704-712.

[14] W. Shi, P. Gong, A new user authentication protocol for wireless sensor networks using elliptic curves cryptography, International Journal of Distributed Sensor Networks, 2013 (2013).

[15] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors, 14 (2014) 10081-10106.